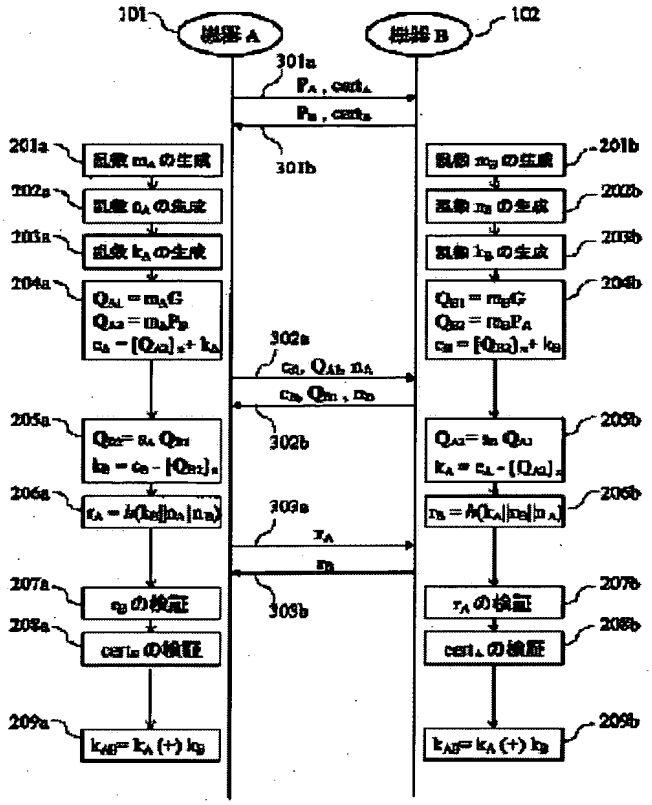
OTHER PARTY AUTHENTICATION AND KEY DELIVERY METHOD, DEVICE USING THE METHOD, CRYPTOGRAPHY COMMUNICATION METHOD AND SYSTEM THEREFOR

Publication number: JP11234259
Publication date: 1999-08-27
Inventor: AIKAWA SHIN; TAKARAGI KAZUO
Applicant: HITACHI LTD
Classification:
- international: ***G09C1/00; H04L9/08; H04L9/32;*** **G09C1/00; H04L9/08; H04L9/32;** (IPC1-7): H04L9/08; G09C1/00; H04L9/32
- european:
Application number: JP19980031635 19980213
Priority number(s): JP19980031635 19980213

Report a data error here

Abstract of **JP11234259**

PROBLEM TO BE SOLVED: To improve the efficiency of other party authentication and key deliv ery by preparing a response by mutually using an irreversible compression function (a hash function) or a common key cryptography based on random numbers of the other party and by mutually exchanging its response. SOLUTION: Equipment A101 calculates a response rA based on rA=h (KB&verbar &verbar nA&verbar &verbar nB) by using random numbers kB, nA and nB. An arithmetic operation X&verbar &verbar Y denotes that bit sequences X and Y are connected and a function h(X) denotes a hash function. Next, the equipment A101 transmits the response rA to equipment B102. Similarly, the equipment B102 transmits a response rB to the equipment A101. Next, the equipment A101 calculates h(kA&verbar &verbar nB) by using random numbers kA, nA and nB and verifies that the result is equal to the response rB received from the equipment B102. Then, the equipment A101 verifies a certifier certB of the equipment B102 by using a public key PLA of a key management organization 131. When the verification result is correct, the equipment A101 cortifies that the equipment B102 is the right equipment.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－234259

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｃ
Ｇ０９Ｃ	1/00	６２０	Ｇ０９Ｃ	1/00	６２０Ｚ
		６４０			６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－31635

(22)出願日　平成10年(1998)２月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　相川　慎
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

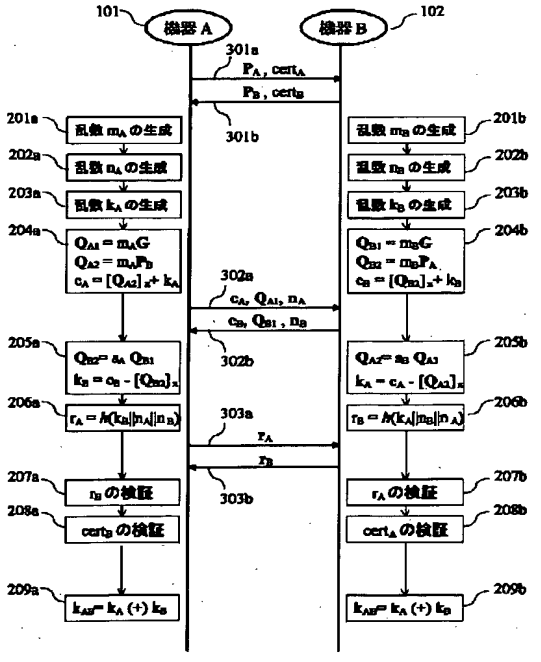
(54)【発明の名称】　相手認証と鍵配送方法とそれを用いた装置、および、暗号通信方法と暗号通信システム

(57)【要約】

【課題】楕円曲線上の演算回数が少なく高速処理が可能な、相手認証と鍵配送方法を提供すること。

【解決手段】機器Aが、機器Bの公開鍵PBを楕円曲線上の演算によって乱数mA倍する処理1と、機器Bが、機器Aの公開鍵PAを楕円曲線上の演算によって乱数mB倍する、処理1と平行した処理2と、機器Aが、機器Bから送信される楕円曲線上の点QB1を、機器Aの秘密鍵sAを用いて楕円曲線上の演算によってsA倍する処理3と、機器Bが、機器Aから送信される楕円曲線上の点QA1を、機器Bの秘密鍵sBを用いて楕円曲線上の演算によってsB倍する、処理3と平行した処理4と、機器Aが、処理3を含む演算結果として得られるデータkBをハッシュ関数または共通鍵暗号で変換して得られるデータrAを機器Bに送信する処理5と、機器Bが、処理4を含む演算結果として得るデータkAをハッシュ関数または共通鍵暗号で変換して得るデータrBを機器Aに送信する処理6とを含む。

図 2



1

【特許請求の範囲】

【請求項１】２つの機器Aと機器Bの間で、相手機器の正当性を確認し、共通の鍵を共有するために行う、相手認証および鍵配送方法であって、

前記機器Aが、前記機器Bの公開鍵PBを、楕円曲線上の演算によって、乱数mA倍する処理1と、

前記機器Bが、前記機器Aの公開鍵PAを、楕円曲線上の演算によって、乱数mB倍する処理を、前記処理1と並行して行う処理2と、

前記機器Aが、前記機器Bから送信される、楕円曲線上の点QB1を、前記機器Aの秘密鍵sAを用いて、楕円曲線上の演算によって、sA倍する処理3と、

前記機器Bが、前記機器Aから送信される、楕円曲線上の点QA1を、前記機器Bの秘密鍵sBを用いて、楕円曲線上の演算によって、sB倍する処理を、前記処理3と並行して行う処理4と、

前記機器Aが、前記処理3を含む演算結果から得られるデータkBを、ハッシュ関数または共通鍵暗号で変換し、その結果得られるデータrAを前記機器Bに送信する処理5と、

前記機器Bが、前記処理4を含む演算結果から得られるデータkAを、ハッシュ関数または共通鍵暗号で変換し、その結果得られるデータrBを前記機器Aに送信する処理6と、

前記機器Aが、前記データkBを含むデータから、共有鍵kABを生成する処理７と、

前記機器Bが、前記データkAを含むデータから、共有鍵kABを生成する処理8と、

を含むことを特徴とする、相手認証および鍵配送方法。

【請求項２】２つの機器Aと機器Bの間で、相手機器の正当性を確認するために行い、共通の鍵を共有する、相手認証および鍵配送方法であって、

前記機器Aと前記機器Bが、通信を開始する前に、

前記機器Aは、楕円曲線上の点Gを、楕円曲線上の演算によって乱数mA倍する処理9を行い、

前記機器Bは、楕円曲線上の点Gを、楕円曲線上の演算によって乱数mB倍する処理10を行い、

前記機器Aと前記機器Bは、処理9と処理10の後で、通信を開始し、

その後、前記機器Aは、前記処理9の演算結果を用いて、共有鍵kABの生成を行う処理11を行い、

同時に、前記機器Bは、前記処理10の演算結果を用いて、共有鍵kABの生成を行う処理12を行い、

前記処理11と前記処理12の後で、前記機器Aは前記機器Bの公開鍵PBの正当性を検証する処理13を行い、

前記機器Ｂは前記機器Ａの公開鍵PAの正当性を検証する処理14を行うことを特徴とする、相手認証および鍵配送方法。

【請求項３】請求項１または請求項２記載の相手認証および鍵配送方法にであって、

2

前記機器Aが、前記機器Bに、機器Aの公開鍵と、前記機器Aの公開鍵が正しいことを証明する認証子を送る処理と、前記機器Bが、前記機器Aに、機器Bの公開鍵と、前記機器Bの公開鍵が正しいことを証明する認証子を送る処理と、

前記機器Aが、第１の乱数と、第２の乱数を生成し、前記第１の乱数を、前記機器Bの公開鍵を基に、楕円曲線暗号を用いて暗号化して、第１のメッセージを生成する処理と、

前記機器Bが、第３の乱数と、第４の乱数を生成し、前記第３の乱数を、前記機器Aの公開鍵を基に、楕円曲線暗号を用いて暗号化して、第２のメッセージを生成する処理と、

前記機器Aが、前記第２の乱数と、前記第１のメッセージを、前記受信機に送る処理と、

前記機器Bが、前記第４の乱数と、前記第２のメッセージを、前記機器Aに送る処理と、

前記機器Aが、前記第２のメッセージを、機器Aの秘密鍵を基に復号化して、前記第３の乱数を取得し、前記第３の乱数と、前記第２の乱数と、前記第４の乱数を、ハッシュ関数を用いて変換して、第３のメッセージを生成する処理と、前記機器Bが、前記第１のメッセージを、機器Bの秘密鍵を基に復号化して、前記第１の乱数を取得し、前記第１の乱数と、前記第２の乱数と、前記第４の乱数を、前記ハッシュ関数を用いて変換して、第４のメッセージを生成する処理と、

前記機器Aが、前記第３のメッセージを、前記受信機に送る処理と、

前記機器Bが、前記第４のメッセージを、前記機器Aに送る処理と、

前記機器Aが、記第１の乱数と、前記第２の乱数と、前記第４の乱数を、前記ハッシュ関数を用いて変換した結果と、前記第３のメッセージが同値であることを検証する処理と、

前記機器Aが、前記機器Bの認証子が正しいことを検証する処理と、

前記機器Bが、記第３の乱数と、前記第２の乱数と、前記第４の乱数を、前記ハッシュ関数を用いて変換した結果と、前記第１のメッセージが同値であることを検証する処理と、

前記機器Bが、前記機器Aの認証子が正しいことを検証する処理と、

前記機器Aは、前記第１の乱数と、前記第３の乱数を基に、共有鍵を生成する処理と、

前記機器Bは、前記第１の乱数と、前記第３の乱数を基に、共有鍵を生成する処理と、

をことを特徴とする、相手認証および鍵配送方法。

【請求項４】請求項１または請求項２記載の相手認証および鍵配送方法であって、

相手認証処理および共通鍵の生成を行う、認証手段と、

共通鍵暗号による暗号変換を行う、暗号変換手段と、
を有する送信装置と、
前記認証手段と、前記暗号変換手段が行う暗号変換の逆変換を行う、復号変換手段と、
を有する受信機器と、
映画などのコンテンツデータを配信する、コンテンツプロバイダーと、
前記送信機器と前記受信機器の、秘密鍵と公開鍵を管理する、鍵管理機関とを含み、
前記送信機器は、前記コンテンツプロバイダーから配信されたコンテンツデータを、前記共通鍵を用いて、前記暗号変換手段により暗号化して、暗号文データを送信し、
前記受信機器は、前記送信機器から受信した、前記暗号文データを、前記共通鍵を用いて、前記復号変換手段でにより復号化して、元の前記コンテンツデータを得ることを特徴とする、暗号通信システム。

【請求項５】請求項４記載の鍵管理機関において、
楕円暗号に基づいて、前記鍵管理機関の秘密鍵と公開鍵と、前記送信機器の秘密鍵と公開鍵と、前記受信機器の秘密鍵と公開鍵と、を生成する、鍵生成手段と、
前記鍵管理機関の秘密鍵を基に、前記送信機器の公開鍵の正当性を証明する認証子と、前記受信機器の公開鍵の正当性を証明する認証子と、を生成する、認証子生成手段と、
前記鍵管理機関の秘密鍵と公開鍵と、前記送信機器の秘密鍵と公開鍵と認証子と、前記受信機器の秘密鍵と公開鍵と認証子を、保持する、保持手段から成り、
前記送信機器は、鍵管理機関から、前記鍵管理機関の公開鍵と、前記送信機器の秘密鍵と公開鍵と認証子とを、安全に取得し、
前記受信機器は、鍵管理機関から、前記鍵管理機関の公開鍵と、前記受信機器の秘密鍵と公開鍵と認証子とを、安全に取得することを特徴とする請求項４記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータ、情報家電機器等の間で行われるデジタルデータの伝送に関するものである。

【０００２】

【従来の技術】今後発展すると予想されるデジタル情報家電機器においては、デジタルデータの不正な複写を防ぐための暗号技術が必須になる。たとえば、デジタル放送受信機で受信したデジタル映像データを、Ｄ－ＶＨＳ（Digital-VHS）などのデジタル録画機器にデジタル録画する場合、デジタル映像データに著作権があれば、それを保護する必要がある。著作権を保護するためには、デジタル複写の制限を設け、相手認証、映像データの暗号変換などの暗号化手段を用いて、データの改ざんや不正な複写を防止する機能が各装置に必要になる。ここで、相手認証とは、接続相手の機器が正当な機器であることを検証することで、不正な機器による、不正行為を防止する方法である。

【０００３】暗号化手段としての、暗号変換アルゴリズムは、大きく、共通鍵暗号と、公開鍵暗号の、二つに分類される。共通鍵暗号は、暗号化と復号化で同一の鍵を用いる暗号である。これに対して、公開鍵暗号は、暗号化に用いる鍵と、復号化に用いる鍵が異なる暗号である。共通鍵暗号は、公開鍵暗号に比べて、ハードウェアとソフトウェアでの処理速度が速い。上述した映像データの暗号変換は、高速処理を必要とするので、一般に共通鍵暗号が用いられる。しかし、データの暗号変換に共通鍵暗号を用いる場合、受信側と送信側の両者に、事前に、共通の鍵（共通鍵）を秘密に配送する、鍵配送を実行しておく必要がある。

【０００４】公開鍵暗号は、暗号化のための鍵を公開鍵と呼び、関係者に公開する。一方、復号化のための鍵を秘密鍵と呼び、自分だけが秘密に持っておく。公開鍵暗号を用いて、暗号通信を行う場合は以下のようにして行う。まず、送信者は、受信者の公開鍵を取得する。ここで、公開鍵は、秘密にする必要はない。次に、送信者は、受信者の公開鍵を用いて、メッセージを暗号化する。最後に、受信者は、暗号化されたメッセージを、自分の秘密鍵で復号化する。受信者の公開鍵で暗号化したメッセージを、正しく復号化できるのは、秘密鍵を知っている受信者だけなので、暗号通信が成立することになる。このような、公開鍵暗号は、秘密情報（すなわち秘密鍵）を、一個所で秘密に管理しておけばよいので、共通鍵方法に比べて、秘密情報がばれにくい。このため、一般に、公開鍵暗号は、相手認証や鍵配送手段に用いられる場合が多い。

【０００５】公開鍵暗号には、たとえば、Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.に紹介されているようなアルゴリズムがある。ここでは、近年有望視されている楕円曲線暗号について簡単に説明する。楕円暗号とは、1985年にMillerとKoblizによって、それぞれ独立に考案された、公開鍵暗号である。これは、楕円曲線上の点Gのｋ倍点を求めるのは簡単だが、結果のkGという値から、逆にkを推定するのが困難であるという、楕円曲線上の離散対数問題の困難性を拠り所とする。楕円曲線暗号では、整数sをランダムに選び、これを秘密鍵とする。また、ベースポイントと呼ばれる楕円曲線上の定点Gを任意に選び、P=sGを計算し、これを公開鍵とする。上述したように、公開鍵Pとベースポイント Ｇからは、秘密鍵sを推定するのが難しい。

【０００６】公開鍵暗号で相手認証を行う場合、デジタル署名を用いる方法が考えられる。ここで、デジタル署名とは、メッセージが生成された内容と同じであるとい

5

う真正性を保証するのに用いられ、公開鍵暗号によって実現される。デジタル署名は、署名者が自分の秘密鍵を用いて、メッセージを変換することで生成される。検証者は署名者からメッセージとそのデジタル署名を受け取り、デジタル署名を、署名者の公開鍵を用いて変換する。そして、変換結果が、署名者のメッセージと同じであることを検証する。デジタル署名を生成できるのは、正しい秘密鍵を知っている署名者だけなので、これによって、メッセージの真正性を照明できる。デジタル署名としては、たとえば、IEEE1363で標準化されている、楕円曲線暗号を用いた、ECDSA (Elliptic Curve Digital Signature Algorithm)や、ECSS (Elliptic Curve Signature Scheme)が挙げられる。このデジタル署名を以下のような手順で用いることで、相手認証を行うことができる。ここで、認証をされる側を利用者、認証を行う側を検証者と呼ぶものとする。

【０００７】（１）検証者は、乱数ｒを生成し、チャレンジとして利用者に送る。

（２）利用者は、自分の秘密鍵sを用いて、rに対するデジタル署名t = S(s, r)を求め、レスポンスとして検証者に送る。

（３）検証者は、利用者の公開鍵Pを用いて、デジタル署名を変換し、その変換結果がrと等しければ、検証者は、利用者が正当な秘密鍵を持った、正しい利用者であることを認証する。

この方法は、チャレンジ・レスポンス型の相手認証である。この手順を、今度は、検証者と利用者が入れ替わって実行するすれば、相互に相手を認証することができる。

【０００８】鍵配送に関しては、共有したい鍵を、一方で生成し、公開鍵暗号を用いて暗号化して、他方に送る方法がある。あるいは、Diffie-Hellman鍵配送方法と呼ばれる手法がある。これは、離散対数問題の困難性を拠り所としている。 Diffie-Hellman鍵配送方法は、前述した楕円曲線暗号を用いても実現できる。以下、この手順を説明する。図4において、機器A11と機器B12が暗号鍵kABを共有するために、楕円暗号を用いたDiffie-Hellman鍵配送方法を行っている。ここで、機器A11と機器B12の間で、予め共通のベースポイントGを決めておく。まず機器A11は、乱数kAを生成し秘密に保持する（処理21a）。続いて、ベースポイントGを用いてVA = kAGを計算する（処理22a）。同様に、機器B12は、乱数kBを生成し、秘密に保持する（処理21b）。続いて、ベースポイントGを用いてVB = kBGを計算する（処理22b）。次に、機器A11は機器B12にVAを転送する（処理31a）。同様に、機器B12は機器A11にVBを転送する（処理31b）。VAとVBが通信路上に流れたとしても、VAからはkAの値を推測するのが困難であり、VBからはkBの値を推測するのが困難である。次に、機器A11は、VBとkAを用いて、 kAB = kAVBを計算し、これを暗号鍵とする（処理23a）。同

6

様に、機器B12は、VAとkBを用いて、 kAB = kBVAを計算し、これを暗号鍵とする（処理23b）。ここで、 kAB = kAVB =kA (kBG) = kB (kAG) = kBVAが成り立つので暗号鍵の共有が可能になる。

【０００９】

【発明が解決しようとする課題】しかし、楕円曲線暗号は、楕円曲線上の演算kGの計算にかなりの処理時間を要する。上述したデジタル署名ECDSAを用いた、相手認証では、署名作成に1回、署名検証に2回の合計３回行う必要がある。また、楕円Diffie-Hellman鍵配送方法においては、それぞれの機器が、２回ずつ行う必要がある。したがって、ECDSAと楕円Diffie-Hellman鍵配送方法を、民生機器用の低コストのハードウェアに実装し、デジタル機器間の相手認証と鍵配送に用いた場合、リアルタイム性を損なう可能性がある。また、相手認証と、鍵配送をそれぞれ独立した方法を用いて行っていたため、全体としての効率が考慮されていない。

【００１０】本発明の目的は、相手認証と鍵配送とを組み合わせ、相手認証と鍵配送とを効率よく実行する方法と、それを用いた装置を提供することである。具体的な本発明の目的は、上述の、相手認証と鍵配送とを効率よく実行する方法と、それを用いた装置を提供するために、楕円曲線上の演算回数を少なくして処理を高速化することである。また、本発明の他の目的は、リアルタイム性を損なわない高速で安全な相手認証と鍵配送方法を用いた暗号通信方法を提供することである。さらに、上記暗号通信方法を用いた暗号通信システムと、それに用いる個々の装置、すなわち暗号通信に用いる送信装置と受信装置を提供することである。また、上記暗号通信方法を用いた、リアルタイム性を損なわない高速で安全な暗号通信方法を用いたデジタルデータ転送方法とそれを用いたデジタル機器を提供することである。

【００１１】

【課題を解決するための手段】上記目的を達成するために、本発明の認証処理手段は、相互が異なる乱数を楕円暗号で暗号化して交換し、相互が相手の前記乱数を復号化して取得し、これをもとに暗号鍵を共有する。さらに、相互が前記相手の乱数を基に、非可逆的な圧縮関数（ハッシュ関数）または共通鍵暗号を用いることで、レスポンスを作成し、相互が前記レスポンスを交換し、相互に相手の前記レスポンスを検証しあうことで、相手が正当であることを相互に認証する。

【００１２】具体的には、本発明では、機器Aが、機器Bの公開鍵PBを、楕円曲線上の演算によって、乱数mA倍する処理１と、機器Bが、機器Aの公開鍵PAを、楕円曲線上の演算によって、乱数mB倍する処理を、処理１と平行して行う処理２と、機器Aが、機器Bから送信される、楕円曲線上の点QB1を、機器Aの秘密鍵sAを用いて、楕円曲線上の演算によって、sA倍する処理３と、機器Bが、機器Aから送信される、楕円曲線上の点QA1を、機器Bの秘密鍵

7

sBを用いて、楕円曲線上の演算によって、sB倍する処理を、処理３と平行して行う処理4と、機器Aが、処理3を含む演算結果として得られるデータkBを、ハッシュ関数または共通鍵暗号で変換し、その結果得られるデータrAを機器Bに送信する処理５と、機器Bが、処理4を含む演算結果として得られるデータkAを、ハッシュ関数または共通鍵暗号で変換し、その結果得られるデータrBを機器Aに送信する処理6とを設けた。

【００１３】本発明によれば、鍵配送処理の結果を用いて、ハッシュ関数または共通鍵暗号で相手認証処理でのレスポンス作成を行うことができる。これにより、楕円曲線上の演算回数を減らすことができ、処理の高速化が可能になり、上述の目的を達成することが可能になる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。まず、本発明の実施形態に係る、相手認証および鍵配送方法について説明する。図１は、暗号通信を行う二つの機器を示すブロック図である。図１において、機器A101と機器B102は、通信路120を介して接続されている。機器A101は、暗号変換手段103と、認証処理手段A105と、データ処理手段A107と、記憶手段A109とを備える。機器B102は、復号変換手段104と、認証処理手段B106と、データ処理手段B108と、記憶手段B110とを備える。

【００１５】機器A101のデータ処理手段A107は、コンテンツプロバイダー141が配信するコンテンツデータを処理する。本実施例は、本発明の一適用例として、機器A101にデジタル放送受信装置、コンテンツプロバイダー141にデジタル放送サービス提供機関を想定している。この場合、データ処理手段A107は、ＭＰＥＧ２－ＴＳ（Transport Stream)形式のような、デジタル番組データの受信、多重分離、伸長などを行う。また、機器B102は、デジタル録画装置を想定している。この場合、データ処理手段B108は、デジタル番組データの多重分離、伸長、蓄積などを行う。機器A101の暗号変換手段103は、暗号鍵kABを用いて、データ処理手段A107より出力されるコンテンツデータに、共通鍵暗号方法による暗号変換を施し、通信路120上に暗号データを流す。機器B102の復号変換手段104は、暗号変換手段103で暗号変換された、暗号データを暗号鍵kABを用いて復号化して、元のコンテンツデータを得て、データ処理手段B108に入力する。これによって、暗号通信が行われる。

【００１６】ここで、暗号変換手段103と復号変換手段104で用いる暗号鍵を同一の値に設定しておく必要がある。また、暗号通信の前に、各機器がお互いを相手認証しておく必要がある。これらの処理を行うのが、認証処理手段A105および認証処理手段B106である。認証処理手段A105と認証処理手段B106は、楕円曲線暗号を用いた相手認証と暗号鍵の交換(共有)を行う。このとき、認証処理手段A105は、記憶手段A109に保持されている、機器A101の公開鍵PA、秘密鍵sA、認証子certA、および、鍵管理機関の公開鍵PLAを用いる。同様に、認証処理手段B106は、記憶手段B110に保持されている、機器B102の公開鍵PB、秘密鍵sB、認証子certB、および、PLAを用いる。

8

【００１７】各機器が保持する、秘密鍵と公開鍵と認証子は、楕円曲線暗号を基に生成され、鍵管理機関131によって管理される。鍵管理機関131は、鍵生成手段132と認証子生成手段133と保持手段134からなる。鍵生成手段132において、各機器の秘密鍵と公開鍵、および鍵管理機関131の秘密鍵と公開鍵が生成される。秘密鍵と公開鍵の生成方法は、上述した通りである。すなわち、機器A101の秘密鍵sAを定め、楕円曲線上の定点であるベースポイントGを用いて、公開鍵をPA = sA Gと定める。同様に、機器B102および鍵管理機関の秘密鍵をsA 、sLA と定め、同じベースポイントGを用いて、公開鍵をPB = sB G 、PLA = sLA Gと定める。ここで、ベースポイントGの値は隠す必要がなく、公開してもよい。これらの鍵は、保持手段134により秘密に保持される。認証子生成手段133では、各機器の認証子が生成される。各機器の認証子は、各機器の公開鍵のデジタル署名であり、鍵管理機関131の秘密鍵を用いて生成される。認証子の生成方法は、一例として従来の技術で述べた、楕円暗号によるデジタル署名アルゴリズムECDSAに従う。生成された認証子は、保持手段134で保持される。

【００１８】鍵管理機関131は、安全な通信路A121を介して、機器A101に、PA、sA、certA、PLAを転送する。あるいは、機器A101の製造時に記憶手段A109に埋め込んでおいてもよい。同様に、鍵管理機関は、安全な通信路B122を介して、機器B102に、PB、sB、certB、PLAを転送する。あるいは、機器B102の製造時に記憶手段B110に格納しておいてもよい。

【００１９】なお、図1において、記憶手段Ａ１０９，Ｂ１１０は、半導体メモリを用い、たとえば後から上述の情報を記憶する場合は電源バックアップされたＲＡＭ、フラッシュメモリ、ＥＥＰＲＯＭなどの書き込み可能な不揮発メモリを用いることができ、機器の製造時に格納する場合は、上記のほかＲＯＭを使うことができる。さらに、認証処理手段Ａ１０５，Ｂ１０６は、それぞれ1チップマイコンや、プログラムメモリ外付けのMPUなどが以下説明する処理を実現するプログラムを実行することで実現されるものである。さらに、安全な通信路B122の代わりに、ICカードのような記憶媒体を用いても良い。

【００２０】図２は、機器A101の認証処理手段A105と機器B102の認証処理手段B106の間で行われる、相互相手認証のフロー図である。ここで、相手認証は、鍵管理機関が生成した正しい秘密鍵を、相手の機器が保持していることを、その秘密鍵を明かすことなく、検証機器が確認することで行われる。以下、このフロー図を順を追って説明していく。

【００２１】まず、機器Aは、自分の公開鍵PAと認証子certAを機器Bに送る（処理301a）。同様に、機器Bは、自分の公開鍵PBと認証子certBを機器Aに送る（処理301b）。次に、機器A101は、乱数mAの生成（処理201a）、乱数nAの生成（処理202a）、乱数kAの生成（処理203a）を行う。201a～203aの処理順序は制限されない。ここで、乱数mAと乱数kAは機器A101が秘密に保持する。また、乱数nAは、機器B102へのチャレンジである。続いて、機器A101は、乱数kAを機器Bの公開鍵PBを用いて暗号化してcAを生成する（処理204a）。この暗号変換は、楕円曲線暗号を用いる。処理204aの手順は以下の通りである。

【００２２】（１）　乱数mA とベースポイントGから、QA1 = mAG を計算する。

（２）　乱数mA と機器Bの公開鍵PBから、QA2 = mAPB を計算する。

（３）　cA = [QA2] x + kA を計算する。ここで、[QA2] xは点QA2のx座標である。[QA2] xの値が分からなければ、 cAからkAを知ることはできない。

【００２３】同様に、機器B102は、乱数mBの生成（処理201b）、乱数nBの生成（処理202b）、乱数kBの生成（処理203b）を行う。201b～203bの処理順序は制限されない。ここで、乱数mBと乱数kBは機器B101が秘密に保持する。また、乱数nBは、機器A101へのチャレンジである。続いて、機器B101は、乱数kBを機器Aの公開鍵PAを用いて暗号化しcBを生成する（処理204b）。処理204bの手順は、処理204aと同様であり、以下のように行われる。

【００２４】（１）　乱数mB とベースポイントGから、QB1 = mBG を計算する。

（２）　乱数mB と機器Bの公開鍵PAから、QB2 = mBPA を計算する。

（３）　cB = [QB2] x + kB を計算する。ここで、[QB2] xは点QB2のx座標である。[QB2] xの値が分からなければ、cBからkBを知ることはできない。

【００２５】ここで、機器A101が行う処理201a～204aと機器B102が行う処理201b～204bは、それぞれの機器で同時に実行することが可能である。次に、機器A101はcAとnAとQA1を機器B102に送る（処理302a）。同様に、機器B102はcBとnBとQB1を機器A101に送る（処理302b）。次に、機器A101は、cBを、機器Aの秘密鍵sAとQB1を用いて復号化し、kBを取得する（処理205a）。処理205aの手順は以下の通りである。

【００２６】（１）　機器A101の秘密鍵sAとQB1から、QB2 = sAQB1 を得る。この式は、sAQB1 =sA（mBG）= mB（sAG）= mB（PA）= QB2 より成り立つことが分かる。QB2の値は、機器A101と機器B102しか知ることができない。

（２）　kB = cB - [QB2] xを計算する。

【００２７】同様に、機器B102は、cAを、機器B102の秘密鍵sBとQA1を用いて復号化し、kAを取得する（処理205b）。処理205bの手順は，処理205aと同様で、以下の通りである。

【００２８】（１）　機器B102の秘密鍵sBとQA1から、QA2 = sBQA1 を得る。この式は、sBQA1 =sB（mAG）= mA（sBG）= mA（PB）= QA2 より成り立つことが分かる。QA2の値は、機器A101と機器B102しか知ることができない。

（２）　kA = cA - [QA2] xを計算する。

【００２９】次に、機器A101は、kBとnAとnB を用いて、レスポンスrAを以下のように計算する。

rA = h(kB || nA || nB)　（処理206a）

ここで、演算X||Yは、ビット列Xとビット列Yを結合することを表す。また、関数h(X)は、ハッシュ関数である。ハッシュ関数とは、任意長のデータを固定長のデータに圧縮する非可逆的な関数であり、デジタル署名や認証などの目的で広く用いられる。ハッシュ関数の演算負荷は、楕円暗号演算処理の数%しかなく小さいので、本発明の処理速度向上に寄与する。同様に、機器B102は、kAとnAとnBを用いて、レスポンスrBを以下のように計算する。

rB = h(kA || nB || nA)　（処理206b）

ここで、機器A101が行う処理205aおよび206aと、機器B102が行う処理205bと206bは、それぞれの機器で同時に実行することが可能である。また、この処理206a、206bでは、ハッシュ関数を使う代わりに同様に計算負荷が小さい共通鍵暗号を用いても良い。すなわち、nAとnB とを、kAを鍵とした共通鍵暗号を用いてレスポンスrBを作成しても良い。

【００３０】次に、機器A101は、機器B102にレスポンスrAを送る（処理303a）。同様に、機器B102は、機器A101にレスポンスrBを送る（処理303b）。次に、機器A101はkAとnAとnB を用いてh(kA || nB || nA)を計算し、その結果が機器B102から受け取ったレスポンスrBと等しいことを検証する（処理207a）。これによって、機器Aが受け取った、機器B201の公開鍵に対応する秘密鍵を、機器B201が保持していることを認証する。機器B201が秘密鍵sBを保持していなければ、機器B201はkAを取得することができず、したがって、正しいレスポンスrBを生成できない。同様な方法で、機器B102は、機器A101のレスポンスrAを検証する（処理207b）。

【００３１】次に、機器A101は、機器B102の認証子certBを検証する（処理208a）。認証子certBの検証は、一例として従来の技術で説明したデジタル署名アルゴリズムであるECDSAに従い、鍵管理機関131の公開鍵PLAを用いて行われる。これによって、機器A101は、機器B102の公開鍵PBが正しいことを確認する。したがって、処理207aと処理208aの検証結果が共に正しければ、機器A101は機器B102が正しい秘密鍵を持っていることを確認でき、機器A101は機器B102を正しい機器と認証する。もし、処理207aと処理208aの検証結果のどちらかが正しくなけれ

ば、機器A101は機器B102を不正な機器と判断し、認証処理を中止する。

【００３２】同様に、機器B102は、機器A101の認証子certAを検証する（処理208b）。処理208bは処理208aと同様な手法で行われる。機器B102は、処理207bと処理208bの検証結果が共に正しいことを確認することで、機器A101を正しい機器と認証する。もし、処理207bと処理208bの検証結果のどちらかが正しくなければ、機器B102は機器A101を不正な機器と判断し、認証処理を中止する。ここで、機器A101が行う処理207aおよび208aと、機器B102が行う処理207bおよび208bは、それぞれの機器で同時に実行することが可能である。

【００３３】機器A101は、機器B102を認証したら、暗号鍵kABを以下のように生成する。

kAB = kA (+) kAB　　（処理209a）

ここで、演算子(+)は、排他的論理和を表す。

【００３４】同様に、機器B102は、機器A101を認証したら、暗号鍵kABを機器A101と同じ方法で生成する（処理209b）。このように、暗号鍵kABの共有は、前述した相手認証を行うために暗号化して交換し合ったkAとkBを用いるので、改めて楕円曲線上の演算を行う必要がない。

【００３５】以上の手順で、機器A101と機器B102は、相互に相手認証を行い、暗号鍵kABを共有する。この相手認証および鍵配送方法において、機器A101が行う楕円曲線上の演算の回数は、処理204aの暗号変換に２回、処理205aの復号変換に１回、処理208aの認証子の検証に２回の合計５回である。機器B102も同様に５回である。もし、認証子の検証に加えて、相手認証のチャレンジ・レスポンスに、従来の技術で説明した、デジタル署名アルゴリズムECDSAを用い、暗号鍵の共有にDiffie-Hellman鍵配送方法を用いると、それぞれの機器における、楕円曲線上の演算は、レスポンス用の署名作成に１回、この署名の検証に２回、認証子の検証に2回、鍵配送に2回の合計７回必要になる。従って、本発明における、相手認証および鍵配送方法の方が、楕円曲線上の演算回数が少なく、したがって、処理時間が短くなる。

【００３６】なお、認証子の検証は、それぞれ相手の公開鍵の真正性を検証するための処理であり、相手の公開鍵が正しいという前提にたてば省略することも可能である。その際は、楕円曲線上の演算回数が従来方法の5回に比べ、3回で済むことになる。また、処理202bにおいて乱数nBを用いることで、たとえ相手から送られてくるkAとnAとが変化しなくてもレスポンスrBを変化させることができるので、解読攻撃に対して強度を高めることができる。

【００３７】次に、本発明の他の実施例に係る、相手認証および鍵配送方法について説明する。図３は機器A101と機器B102とが行う、相手認証および鍵配送手順のフロー図である。ここで、機器A101と機器B102の構成は、上記実施例で図１を用いて説明した構成と同様であるもの

とする。また、図３において、機器A101が行う処理201a～203aと205a～209a、機器B102が行う処理201b～203bと205b～209bは、上記実施例で図２を用いて説明した処理と同じである。さらに、図３において、機器A101が行う処理401aと処理402aをまとめたものは、図２を用いて説明した処理204aと同じであり、図３において、機器B102が行う処理401bと処理402bをまとめたものは、図２を用いて説明した処理204bと同じである。本実施例の相手認証および鍵配送方法と、上記実施例で説明したものとの相違点は、相手認証および鍵配送処理の前に、乱数の生成と、ベースポイントGを用いた楕円計算を、前処理として行っておくことと、相手認証および鍵配送処理時には、相手からのレスポンスの検証と、相手の公開鍵の正当性を証明する認証子の検証を行わず、相手認証および鍵配送処理後の暗号通信中に、後処理として行うことである。

【００３８】機器Aは、処理201aの乱数mAの生成、処理202aの乱数nAの生成、処理203aの乱数kAの生成、および処理401aのQA1 = mAGの楕円演算を前処理として行っておく。同様に、機器Bは、処理201bの乱数mBの生成、処理202bの乱数nBの生成、処理203bの乱数kBの生成、および処理401bのQB1 = mBGの楕円計算を前処理として行っておく。処理401aと処理401bの楕円演算が前処理として行えるのは、予め分かっているベースポイントGの演算であるからである。機器A101の前処理による計算結果は、図１の記憶手段A109に保持しておく。また、機器B102の前処理による計算結果は、図１の記憶手段B110に保持しておく。この前処理による計算結果を、相手認証および鍵配送処理で用いる。ここで、前処理の計算結果を、記憶手段に複数組保持しておき（これらは、乱数を基に生成されるので、すべて異なった値になる）、相手認証および鍵配送処理時にその中から、任意の組を選んで用いてもよい。さらに、前処理による計算は、機器A101と機器B102の製造時に行い、記憶手段A109と記憶手段B110とに格納しておいてもよい。これらの計算結果への記憶、記憶手段への格納の実現方法は、上記実施例と同様である。

【００３９】相手認証および鍵配送処理で、前処理の計算結果を使いきってしまった場合は、次に相手認証と鍵配送処理を行う場合に備えて、機器の処理に余裕があるときに、前処理を実行して上記記憶手段へ格納しておけばよい。

【００４０】また、図３において、機器A101と機器B102は、処理303aと処理303bで、レスポンスを交換し合った後、すぐに機器A101は処理209aで暗号鍵kABを生成し、同様に機器B102は処理209bで暗号鍵kABを生成する。そして、共有した暗号鍵kABを用いて、暗号通信を開始する。暗号通信開始後に、機器A101は、機器B102のレスポンスrBの検証（処理207a）と、機器B102の認証子certBの検証（処理208a）を、後処理として行う。もし、処理

13

207aと処理208aの検証結果のどちらかが正しくなければ、機器A101は機器B102を不正な機器と判断し、直ちに暗号通信を中止する。同様に、機器B102は、機器A101のレスポンスrAの検証（処理207b）と機器A101の認証子certAの検証（処理208b）を，後処理として、暗号通信開始後に行う。もし、処理207bと処理208bの検証結果のどちらかが正しくなければ、機器B102は機器A101を不正な機器と判断し、直ちに暗号通信を中止する。ここで、認証子は上記実施例と同様にECDSAを用いているので、その検証には、２回の楕円計算が必要になる。認証子の検証には、上述のようにECSSを使うこともできる。

【００４１】本実施例の相手認証と鍵配送方法は、相手認証と鍵配送を行うために実行する楕円計算を、前処理およびとして１回行い、後処理として２回行うので、上記実施例の相手認証および鍵配送方法に比べて、より短い処理時間で実行することができ、相手認証および鍵配送処理のさらなる高速化が可能になる。

【００４２】

【発明の効果】本発明によれば、相手認証および鍵配送方法において、相手認証および鍵配送処理時に行う、楕円曲線上の演算回数が少なく、高速処理が可能な、相手認証および鍵配送を実現することができる。

【図面の簡単な説明】

【図１】本発明の実施例に係る、暗号通信を行う機器のシステムブロック図である。

14

【図２】本発明の実施例に係る、相手認証および鍵配送方法の手順を示すフロー図である。

【図３】本発明の他の実施例に係る、相手認証および鍵配送方法の手順を示すフロー図である。

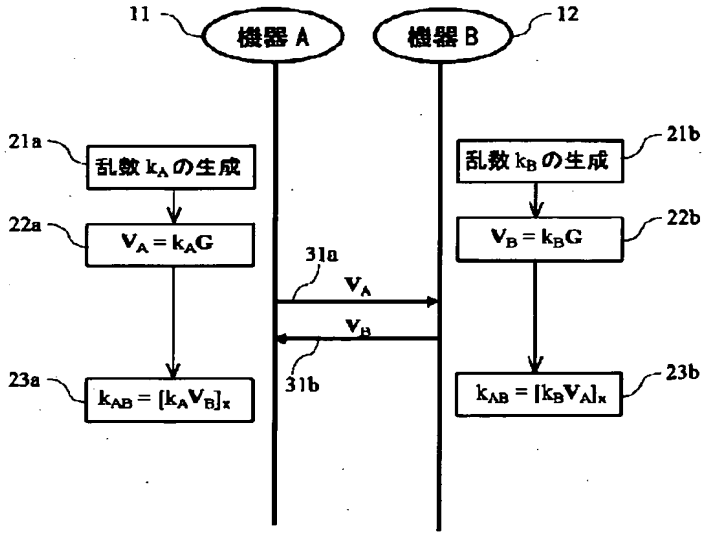
【図４】楕円暗号を用いた、Diffe-Hellman鍵配送方法の手順を示すフロー図である。

【符号の説明】

101･･･機器A、
102･･･機器B、
103･･･暗号変換手段、
104･･･復号変換手段、
105･･･認証処理手段A、
106･･･認証処理手段B、
107･･･データ処理手段A、
108･･･データ処理手段B、
109･･･記憶手段A、
110･･･記憶手段B、
121･･･通信路、
131･･･鍵管理機関、
132･･･鍵生成手段、
133･･･認証子生成手段、
134･･･保持手段。

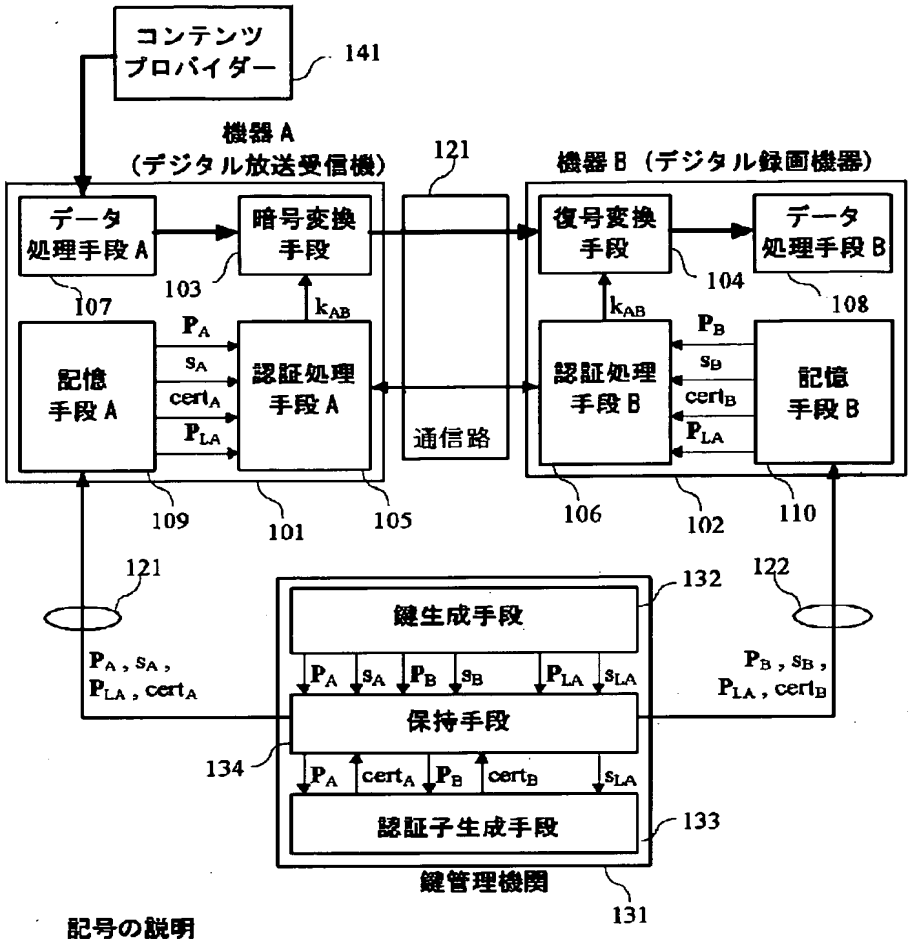
【図４】

図 4



【図１】

図　1

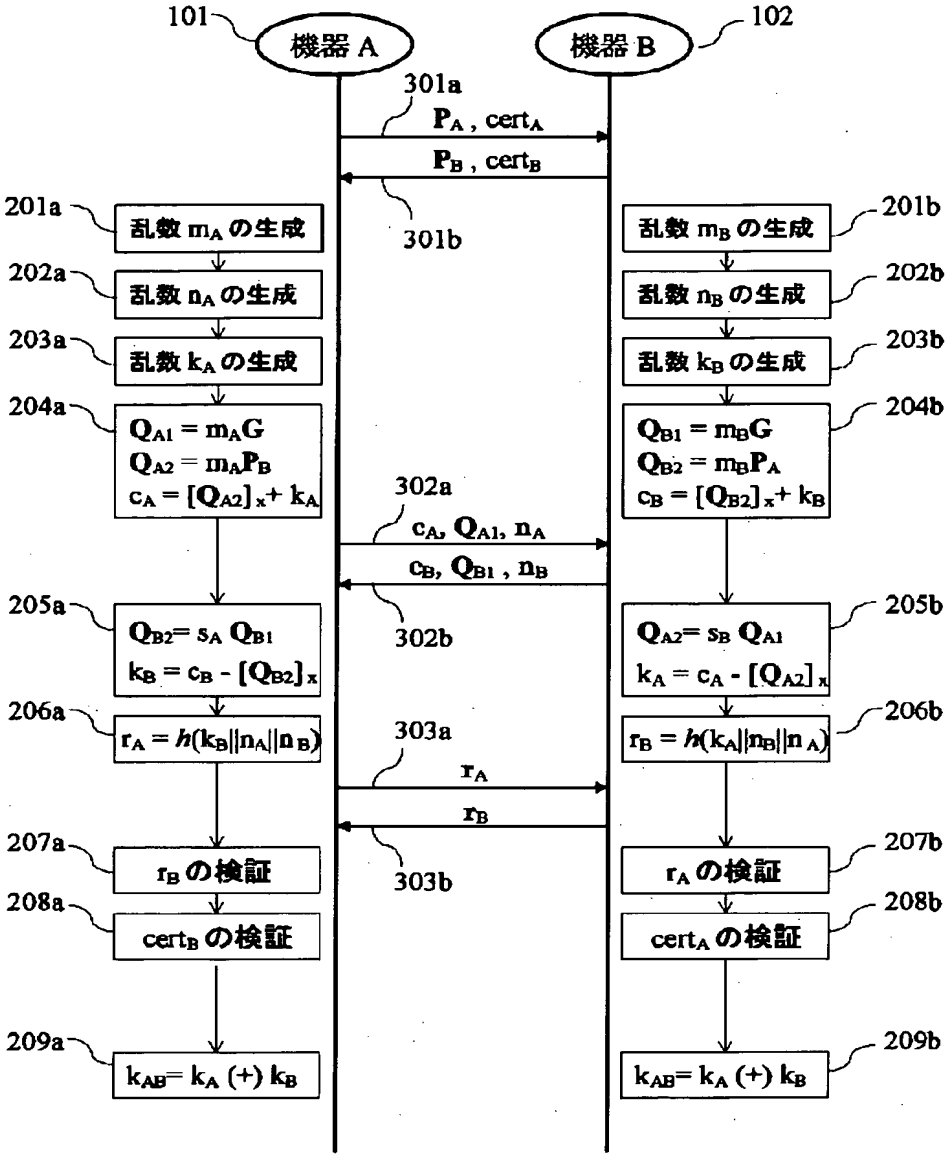


記号の説明

P_A　：機器 A の公開鍵
s_A　：機器 A の秘密鍵
P_B　：機器 B の公開鍵
s_B　：機器 B の秘密鍵
P_{LA}　：鍵管理機関の公開鍵
s_{LA}　：鍵管理機関の秘密鍵
$cert_A$：機器 A の公開鍵の認証子
$cert_B$：機器 B の公開鍵の認証子
k_{AB}　：暗号鍵

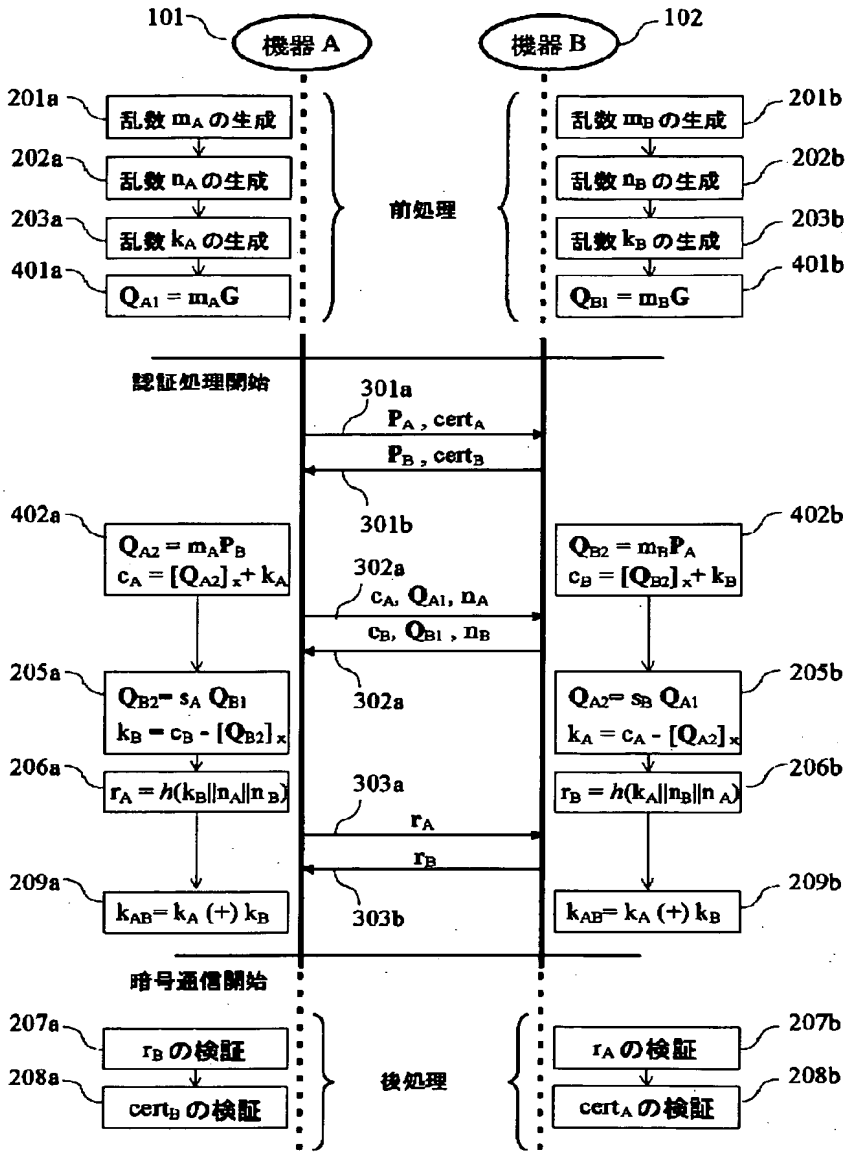
【図２】

図 2


101
機器 A
102
機器 B
301a
P_A , $cert_A$
P_B , $cert_B$
301b
201a
乱数 m_A の生成
201b
乱数 m_B の生成
202a
乱数 n_A の生成
202b
乱数 n_B の生成
203a
乱数 k_A の生成
203b
乱数 k_B の生成
204a
$Q_{A1} = m_A G$
$Q_{A2} = m_A P_B$
$c_A = [Q_{A2}]_x + k_A$
204b
$Q_{B1} = m_B G$
$Q_{B2} = m_B P_A$
$c_B = [Q_{B2}]_x + k_B$
302a
c_A, Q_{A1}, n_A
c_B, Q_{B1} , n_B
302b
205a
$Q_{B2} = s_A Q_{B1}$
$k_B = c_B - [Q_{B2}]_x$
205b
$Q_{A2} = s_B Q_{A1}$
$k_A = c_A - [Q_{A2}]_x$
206a
$r_A = h(k_B || n_A || n_B)$
303a
206b
$r_B = h(k_A || n_B || n_A)$
r_A
r_B
303b
207a
r_B の検証
207b
r_A の検証
208a
$cert_B$ の検証
208b
$cert_A$ の検証
209a
$k_{AB} = k_A$ (+) k_B
209b
$k_{AB} = k_A$ (+) k_B

【図３】

図 3


101
機器 A
102
機器 B
201a
乱数 m_A の生成
202a
乱数 n_A の生成
203a
乱数 k_A の生成
401a
$Q_{A1} = m_A G$
前処理
201b
乱数 m_B の生成
202b
乱数 n_B の生成
203b
乱数 k_B の生成
401b
$Q_{B1} = m_B G$
認証処理開始
301a
P_A , $cert_A$
P_B , $cert_B$
301b
402a
$Q_{A2} = m_A P_B$
$c_A = [Q_{A2}]_x + k_A$
302a
c_A, Q_{A1}, n_A
c_B, Q_{B1} , n_B
302a
402b
$Q_{B2} = m_B P_A$
$c_B = [Q_{B2}]_x + k_B$
205a
$Q_{B2} = s_A Q_{B1}$
$k_B = c_B - [Q_{B2}]_x$
205b
$Q_{A2} = s_B Q_{A1}$
$k_A = c_A - [Q_{A2}]_x$
206a
$r_A = h(k_B \| n_A \| n_B)$
303a
r_A
r_B
303b
206b
$r_B = h(k_A \| n_B \| n_A)$
209a
$k_{AB} = k_A (+) k_B$
209b
$k_{AB} = k_A (+) k_B$
暗号通信開始
207a
r_B の検証
208a
$cert_B$ の検証
後処理
207b
r_A の検証
208b
$cert_A$ の検証